REMARKS

The Examiner has objected to the specification for failing to provide proper antecedent basis for the claimed subject matter of claim 39. Applicant respectfully asserts that such objection is deemed moot in view of the cancellation made to the claim hereinabove.

The Examiner has further objected to the amendment filed 05/10/2006 under 35 U.S.C. 132(a) because it introduces new matter into the disclosure, namely "wherein said updating does not use new secret information." The Examiner has required applicant to cancel such new matter. While applicant respectfully disagrees with the Examiner's assertion, applicant has cancelled the claims associated with such claim language.

The Examiner has rejected Claims 1-9, 11, 12, 28-30 and 38-41 under 35 U.S.C. 112, first paragraph, as failing to comply with the written description requirement. Applicant respectfully asserts that such rejection is deemed moot in view of the amendment made hereinabove to Claim 41 and the cancellations made to the remaining rejected claims hereinabove.

The Examiner has rejected Claim 39 under 35 U.S.C. 101, as being directed to non-statutory subject matter. Applicant respectfully asserts that such rejection is deemed moot in view of the cancellation made to the claim hereinabove.

The Examiner has rejected Claims 1-8, 11-15, 17-21, 28-30 and 38-41 under 35 U.S.C. 102(b) as being anticipated by Balenson et al. ("Dynamic Cryptographic Context Management (DCCM): Report #1 Architecture and System Design"). Applicant respectfully disagrees with such rejection.

With respect to independent claim 13, the Examiner has relied on page 99 from the Balenson reference, excerpted in part below, to make a prior art showing of applicant's claimed technique "wherein said determining uses a function having the

following properties: (1) knowledge of said updated first key does not give knowledge of said first key or said second key,...and (3) knowledge of said first key and said updated first key does not give any knowledge of said second key."

> "The information-theoretic approaches are motivated by two goals: to avoid 'zero-basing' (changing and rebroadcasting) the group key to all group members, and basing security on (unconditional) information-theoretic security rather than on computationally-based security of unproven cryptographic operators. To avoid zero-basing, the information-theoretic methods predistribute secret information to each group member. When a member is evicted, the remaining group members can use this predistributed information to compute a new key, without any trusted controller separately transmitting the new key. The simplest example of this principle is the so-called complementary variables method. The major disadvantage of the information-theoretic approaches is that, in order to prevent collusion by two or more evicted members, a large amount of information must be predistributed (see Section 0)." (Balenson, pg. 99 - emphasis added)

Applicant respectfully points out that the Balenson reference excerpt relied upon by the Examiner merely teaches that "in order to prevent collusion by two or more evicted members, a large amount of information must be predistributed" (Balenson, pg. 99 – emphasis added). In particular, such excerpt from Balenson discloses that "[w]hen a member is evicted, the remaining group members can use this predistributed information to compute a new key, without any trusted controller separately transmitting the new key" (emphasis added).

However, applicant respectfully asserts that only generally disclosing that "a large amount of information must be predistributed," such that "remaining group members can use this predistributed information to compute a new key," as in Balenson, does not specifically teach that "said determining uses a function having the following properties: (1) knowledge of said updated first key does not give knowledge of said first key or said second key," and "(3) knowledge of said first key and said updated first key does not give any knowledge of said second key," as claimed by applicant. In particular, simply disclosing the use of predistributed information to compute a new key, as in Balenson, does not suggest, and especially does not rise to the level of specificity of, applicant's claim language, namely that "knowledge of said updated first key does not give

knowledge of said first key or said second key...and...knowledge of said first key and said updated first key does not give any knowledge of said second key" (emphasis added), as claimed.

The Examiner is reminded that a claim is anticipated only if each and every element as set forth in the claim is found, either expressly or inherently described in a single prior art reference. *Verdegaal Bros. v. Union Oil Co. Of California*, 814 F.2d 628, 631, 2 USPQ2d 1051, 1053 (Fed. Cir. 1987). Moreover, the identical invention must be shown in as complete detail as contained in the claim. *Richardson v. Suzuki Motor Co.*868 F.2d 1226, 1236, 9USPQ2d 1913, 1920 (Fed. Cir. 1989). The elements must be arranged as required by the claim.

This criterion has simply not been met by the Balenson reference excerpt, as noted above. Thus, a notice of allowance or specific prior art showing of each of the foregoing claim elements, in combination with the remaining claimed features, is respectfully requested.

Still yet, applicant brings to the Examiner's attention the subject matter of new Claims 42-50, which are added for full consideration. In particular, applicant has added new Claims 43-50, which provide for an apparatus with limitations similar (but not necessarily identical) to those of Claims 13-15 and 17-21. In addition, applicant has added new Claim 42 as follows:

"wherein said subgroup is a self-repairing group, each member of said subgroup capable of independently updating said first key, where said self-repairing uses a reusable power set, said reusable power set using a power set of said members as a basis for group key updates and including 2^N sets, where N includes the number of said members" (see Claim 42).

Again, a notice of allowance or a proper prior art showing of all of applicant's claim limitations, in combination with the remaining claim elements, is respectfully requested.

Thus, all of the independent claims are deemed allowable. Moreover, the remaining dependent claims are further deemed allowable, in view of their dependence on such independent claims.

In the event a telephone conversation would expedite the prosecution of this application, the Examiner may reach the undersigned at (408) 505-5100. The Commissioner is authorized to charge any additional fees or credit any overpayment to Deposit Account No. 50-1351 (Order No. NAI1P089).

Respectfully submitted,
Zilka-Kotab, PC

/KEVINZILKA/

Kevin J. Zilka
Registration No. 41,429

P.O. Box 721120
San Jose, CA 95172-1120
408-505-5100